WHAT IS CLAIMED IS:

1. A content distribution system for performing content transaction management, comprising:

a plurality of user devices among which the content transaction management allows a content to be secondarily distributed;

a secure container containing the content encrypted by a content key, and container information including conditions set for a transaction of the content;

a first section for distributing the content by transmitting said secure container; and

a second section for performing personal authentication, when said secure container is transmitted among said plurality of user devices, based on a personal identification certificate (hereinafter, simply referred to as an IDC) which is identified in reference to an IDC identifier list,

wherein the container information includes the IDC identifier list as a list of the IDCs, each of which is generated by a personal identification authority (hereinafter, simply referred to as an IDA) as a third party agent and stores a template serving as personal identification data of a target user for the content transaction.

2. The content distribution system according to Claim 1,

wherein a secure container receiving device among said plurality of user devices generates usage control status information on a content based on the container information included in said secure container, and stores the usage control status information in a memory of the receiving device, and further the usage control status information includes the IDC identifier list.

3. The content distribution system according to Claim 1,

wherein a secure container receiving device among said plurality of user devices generates usage control status information on a content based on the container information included in said secure container, and stores the usage control status information in a memory of the receiving device, and further the usage control status information includes conditions set for processing secondary distribution of the content after a primary content distribution.

4. The content distribution system according to Claim 1,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process personal authentication of a user of a receiving device among said plurality of user devices, to which the secure container is to be distributed, and to perform a process so that a content is available at the receiving device, when the comparison result is affirmative.

5. The content distribution system according to Claim 1,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process personal authentication of a user of a receiving device among sail plurality of user devices, to which the secure container is to be distributed, and to perform a process of distribution of the content key for encrypting the content stored in said secure container, when the comparison result is affirmative.

6. The content distribution system according to Claim 1,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process personal authentication of a user of

the receiving device, to which the secure container is to be distributed, and to notify a distributing device among said user devices, as a distributor of said secure container, of the process result of the personal authentication, and further the distributing device is configured to perform a process so that a content is available at the receiving device, when the comparison result is affirmative.

7. The content distribution system according to Claim 1,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process personal authentication of a user of the receiving device, to which the secure container is to be distributed, and to notify a distributing device among said user devices, as a distributor of said secure container, of the process result of the personal authentication, and further the distributing device is configured to perform processes so that said secure container and the content key stored in said secure container are distributed to the receiving device of said secure container and available at the receiving device, when the comparison result is affirmative.

8. The content distribution system according to Claim 1,

wherein the IDC used for personal authentication, which is performed when said secure container is transmitted among said plurality of user devices, is configured to be stored in advance in any of said plurality of user devices which is to perform the personal authentication.

9. The content distribution system according to Claim 1,

wherein any of said user devices, which is to perform personal authentication when said secure container is transmitted among said plurality of user devices, is configured to obtain the IDC used for the personal authentication from the IDA as an issuer of the IDCs.

10. The content distribution system according to Claim 1,

wherein the container information further includes usage permission data of the content such as reproduction and duplication of the content, and a receiving device among said plurality of user devices is configured to perform restricting usage of the content based on the usage permission data of the content or usage control status information generated according to said usage permission data.

11. The content distribution system according to Claim 1,

wherein said secure container further is configured to include a digital signature of a producer of said secure container.

12. The content distribution system according to Claim 1,

wherein the IDC identifier list is configured to include data for associating a user identifier with his/her IDC identifier.

13. The content distribution system according to Claim 1,

wherein each of distributing and receiving devices among said plurality of user devices, which are to perform a content transaction, further comprises an encryption unit, so that each of the devises is configured to perform mutual authentication upon performing data transmission between the distributing and receiving devices, and further the data transmitting and receiving sides are configured, respectively, to generate a digital signature of the transmitting data and to verify the digital signature.

14. The content distribution system according to Claim 1,

wherein the template comprises at least any one of the following (a) to (d): (a) personal biotic information including fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information; (b) personal non-biotic

information including a seal, a passport, a driver's license, and a card; (c) combined information between the biotic information and the non-biotic information; and (d) another combined information of a password and either of (a) and (b).

15. A content distribution method for performing content transaction management for allowing a content to be secondarily distributed among a plurality of user devices, comprising the steps of:

distributing the content by transmitting a secure container containing the content encrypted by a content key, and container information including conditions set for a transaction of the content; and

performing personal authentication, when the secure container is transmitted among the plurality of user devices, based on an IDC which is identified in reference to an IDC identifier list,

wherein the container information contains the IDC identifier list as a list of the IDCs storing a template, each IDC serving as identification data of a target user for the content transaction.

16. The content distribution method according to Claim 15, wherein the IDC is generated by an IDA serving as a third party agent.

17. The content distribution method according to Claim 15,

wherein a secure container receiving device among the plurality of user devices comprises the steps of:

generating usage control status information on a content based on the container information included in the secure container; and

storing the usage control status information in a memory of the receiving device,

besides the status information includes the IDC identifier list

18. The content distribution method according to Claim 15,

wherein a secure container receiving device among the plurality of user devices comprises the steps of:

generating the usage control status information on a content based on the container information included in said secure container; and

storing the usage control status information in a memory of the receiving device,

besides the usage control status information includes conditions set for processing secondary distribution of the content after a primary content distribution.

19. The content distribution method according to Claim 15,

wherein a secure container distributing device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of a receiving device among the plurality of user devices, to which the secure container is to be distributed; and

performing a process so that a content is available at the receiving device, when the comparison result is affirmative.

20. The content distribution method according to Claim 15,

wherein a secure container distributing device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of a receiving device among the plurality of user devices, to which the secure container is to be distributed; and

performing distribution of the content key for encrypting the content stored in the secure container, when the comparison result is affirmative.

21. The content distribution method according to Claim 15,

wherein a secure container receiving device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of the receiving device, to which the secure container is to be distributed; and

notifying a distributing device among the user devices, as a distributor of said secure container, of the result of personal authentication,

besides the distributing device comprises the step of performing a process so that a content is available at the receiving device, when the comparison result is affirmative.

22. The content distribution method according to Claim 15,

wherein a secure container receiving device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of the receiving device, to which the secure container is to be distributed; and

notifying a distributing device among the user devices, as a distributor of the secure container, of the result of personal authentication,

besides the distributing device comprises the step of performing distribution of the secure container and the content key stored in the secure container for encrypting the content to the receiving device of the secure container, when the comparison result is affirmative.

23. The content distribution method according to Claim 15,

wherein the IDC used for personal authentication, which is performed when the secure container is transmitted among the plurality of user devices, is stored in advance in any of the plurality of user devices which is to perform the personal authentication.

24. The content distribution method according to Claim 15,

wherein any of the plurality of user devices, which is to perform personal authentication when the secure container is transmitted among the plurality of user devices, comprises the step of obtaining the IDC necessary for the personal authentication from the IDA as an issuer of the IDCs.

25. The content distribution method according to Claim 15,

wherein the container information further includes usage permission data of the content such as reproduction and duplication of the content, and a receiving device among the plurality of user devices comprises the step of performing restricting usage of the content based on the usage permission data of the content or the usage control status information generated according to said usage permission data.

26. The content distribution method according to Claim 15,

wherein each of content transacting user devices among the plurality of user devices includes an encryption unit and comprises the step of performing mutual authentication upon

performing data transmission among the content transacting user devices, besides data transmitting and receiving sides comprise the steps of, respectively, generating a digital signature of the transmitting data and verifying the digital signature.

27. An information processing apparatus for reproducing a content stored in a storage device, comprising:

a storing section for storing the content in the apparatus when a secure container, including the content encrypted by a content key and container information containing conditions set for a sales price as well as a sales restriction of the content, is transmitted; and

a processing section for performing personal authentication based on an IDC identified in reference to an IDC identifier list when the content is regenerated,

wherein a template serves as identification data of a target user for a content transaction, and the container information includes the IDC identifier list as a list of the IDCs storing the template, each IDC being generated by an IDA serving as a third party agent.

28. The information processing apparatus according to Claim 27, wherein said processing section, further comprising:

a first processing sub-section for performing the personal authentication by comparing the template stored in the IDC identified in reference to the IDC identifier list with sampling information input by a user.

29. The information processing apparatus according to Claim 27, wherein said processing section, further comprising:

a second processing sub-section for performing the personal authentication of a user who is to be permitted to access the information processing apparatus, based on a device-dependent IDC set to the apparatus; and

a third processing sub-section for performing the personal authentication based on the IDS storing the container information and identified in reference to the IDC list, when said secure container is used, in addition to the second processing section being performed.

30. A program providing medium, storing a program which comprises the steps of:

executing a content distribution process for performing content transaction management so that a content is secondarily distributed among a plurality of user devices; and

executing a personal authentication based on an IDC identified in reference to a IDC identifier list when a secure container is transmitted among the plurality of user devices,

wherein the secure container contains the content encrypted by a content key, and container information including conditions set for a transaction of the content as well as the IDC identifier list serving as a list of the IDCs storing a template, each IDC serving as identification data of a target user for the content transaction.

ABSTRACT OF THE DISCLOSURE

A content distribution is performed by a secure container including a content encrypted by a content key and container information set for a content transaction. The container information includes a personal identification certificate identifiers list. Usage control status information including the list is generated and stored in a device during a secondary distribution among user devices after a primary distribution of the content. In the distribution among the user devices, identifying an identification certificate in reference to the list and performing a personal authentication based on the identification certificate allows each of the user terminals to use the transmitted content, when the authentication is affirmative.